

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 53080
	:	
Makoto FUJIWARA, et al.	:	Confirmation Number: 5601
	:	
Application No.: 10/696,621	:	Group Art Unit: 2436
	:	
Filed: October 30, 2003	:	Examiner: COLIN, Carl G.
	:	
For: PROGRAM UPDATE METHOD AND SERVER		

SUBSTANCE OF INTERVIEW

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REMARKS

Claims 1-8 are pending in this application, with claim 1 being independent. Applicants thank Examiner Colin for the thoughtful courtesies and kind treatments afforded to the Applicants' representative during the telephonic interviews conducted on February 10, 2009 and on February 26, 2009.

During the interview conducted on February 10, 2009, Examiner Colin mentioned that the above-identified application will be placed in condition for allowance if claim 1 is amended to recite determining whether updating the program was successfully performed, and deleting old program from a secure memory and writing information about the update object program into the secure memory if it is determined that updating the program was successfully performed. In reliance on this assertion and to expedite prosecution, Applicants authorize Examiner Colin to amend claim 1 (via Examiner's amended) to recite this feature. For ease of reference, a copy of amended claim 1 is provided in the attached Appendix A.

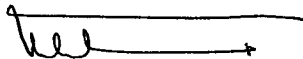
During the interview conducted on February 26, 2009, Examiner Colin suggested revising claim 1 to further clarify the step of "determining whether updating the program was successfully performed." Applicants' representative disagreed and asserted that such amendments would unnecessarily narrow the scope of claim 1. The Examiner subsequently agreed that such a recitation is not necessary.

If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicants' attorney at the telephone number shown below. Based on the foregoing, Applicants believe that this application is in condition for allowance.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Babak Akhlaghi
Limited Recognition No. L0250

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 BA:MaM
Facsimile: 202.756.8087
Date: February 27, 2009

**Please recognize our Customer No. 53080
as our correspondence address.**

APPENDIX A

1. (Currently amended) A method for updating a program in a system including an LSI device and an external memory, the method comprising:

a step of transmitting by the system an ~~inherent~~ ID, which is implemented before the program update, of the LSI device and an application ID which is identification information of an update object program to a server;

a step of determining by the server whether or not the update object program may be transmitted based on the transmitted ~~inherent~~ ID and application ID, and transmitting by the server additional information of the update object program if it is determined that the update object program may be transmitted;

a step of determining by the system whether or not program update is possible based on the transmitted additional information, and requesting by the system that the server to transmit a common key-encrypted program generated by encryption with a common key if it is determined that program update is possible;

a step of receiving by the system the common key-encrypted program transmitted from the server;

a step of decrypting by the system the received common key-encrypted program to generate a raw program; [[and]]

a step of re-encrypting by the system the raw program with an inherent key unique to the LSI device and storing the re-encrypted program in the external memory as a new inherent key-encrypted program;

a step of determining whether updating the program was successfully performed; and

a step of deleting old program from a secure memory and writing information about the update object program into the secure memory if it is determined that updating the program was successfully performed.

2. (Previously presented) The program update method of claim 1, further comprising the steps of:

receiving by the system common key information transmitted from the server; and
generating by the system a raw common key using the received common key information,

wherein at the decrypting step, the raw common key is used to decrypt the common key-encrypted program.

3. (Original) The program update method of claim 2, wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key.

4. (Previously presented) The program update method of claim 1, wherein:
the LSI device includes an internal memory in which inherent key information is stored;
the system uses the inherent key information stored in the internal memory to generate a raw inherent key at boot-up of the system; and

at the re-encrypting step, the raw inherent key is used for re-encrypting the raw program.

5. (Original) The program update method of claim 4, wherein the inherent key information includes an encrypted inherent key generated by encrypting the raw inherent key with a raw third intermediate key and an encrypted second intermediate key generated by encrypting the raw third intermediate key with a raw fourth intermediate key.

6. (Original) The program update method of claim 4, wherein the generated raw inherent key is stored in a register of the LSI device and is used for decrypting the inherent key-encrypted program to a raw program for execution of the inherent key-encrypted program.

7. (Original) The program update method of claim 1, wherein:
the LSI device includes a boot ROM in which a boot program is stored;
the external memory includes an acquisition program for establishing data transmission between the LSI device and a server; and
the system executes reception of the common key-encrypted program based on the acquisition program stored in the external memory, and controls update processing performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM.

8. (Previously presented) The program update method of claim 1, further comprising the step of receiving a HASH value of the raw program transmitted from the server,
wherein at the decrypting step, the received HASH value is used to perform a HASH verification on the decrypted raw program.

Application No.: 10/696,621

9-11. (Cancelled)

INTERVIEW SUMMARY

To: Examiner Colin, Art Unit 2436
From: Mr. Babak Akhlaghi
Re: Claim Amendments
U.S. Patent Application Serial Number 10/696,621
Our reference: 060188-0694

Examiner Colin,

Applicants thank you for the thoughtful courtesies and kind treatments that you afforded to me during the telephonic interview conducted on February 10, 2009. During the interview, you mentioned that the above-identified application will be placed in condition for allowance if claim 1 is amended to recite determining whether updating the program was successfully performed, and deleting old program from a secure memory and writing information about the update object program into the secure memory if it is determined that updating the program was successfully performed.

In reliance on this assertion and to expedite prosecution, Applicants authorize you to amend claim 1 (via Examiner's amended) to recite this feature. For your ease of reference, a copy of amended claim 1 is provided in the attached Appendix A. If there are any outstanding issues that might be resolved by an additional interview or an Examiner's amendment, please call me at the telephone number shown below.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Babak Akhlaghi
Limited Recognition No. L0250
Telephone: 202-756-8327

APPENDIX A

1. (Currently amended) A method for updating a program in a system including an LSI device and an external memory, the method comprising:

a step of transmitting by the system an ~~inherent~~ ID of the LSI device and an application ID which is identification information of an update object program to a server;

a step of determining by the server whether or not the update object program may be transmitted based on the transmitted ~~inherent~~ ID and application ID, and transmitting by the server additional information of the update object program if it is determined that the update object program may be transmitted;

a step of determining by the system whether or not program update is possible based on the transmitted additional information, and requesting by the system that the server to transmit a common key-encrypted program generated by encryption with a common key if it is determined that program update is possible;

a step of receiving by the system the common key-encrypted program transmitted from the server;

a step of decrypting by the system the received common key-encrypted program to generate a raw program; [[and]]

a step of re-encrypting by the system the raw program with an inherent key unique to the LSI device and storing the re-encrypted program in the external memory as a new inherent key-encrypted program;

determining whether updating the program was successfully performed; and

deleting old program from a secure memory and writing information about the update object program into the secure memory if it is determined that updating the program was successfully performed.

2. (Previously presented) The program update method of claim 1, further comprising the steps of:

receiving by the system common key information transmitted from the server; and
generating by the system a raw common key using the received common key information,

wherein at the decrypting step, the raw common key is used to decrypt the common key-encrypted program.

3. (Original) The program update method of claim 2, wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key.

4. (Previously presented) The program update method of claim 1, wherein:
the LSI device includes an internal memory in which inherent key information is stored;
the system uses the inherent key information stored in the internal memory to generate a raw inherent key at boot-up of the system; and

at the re-encrypting step, the raw inherent key is used for re-encrypting the raw program.

5. (Original) The program update method of claim 4, wherein the inherent key information includes an encrypted inherent key generated by encrypting the raw inherent key with a raw third intermediate key and an encrypted second intermediate key generated by encrypting the raw third intermediate key with a raw fourth intermediate key.

6. (Original) The program update method of claim 4, wherein the generated raw inherent key is stored in a register of the LSI device and is used for decrypting the inherent key-encrypted program to a raw program for execution of the inherent key-encrypted program.

7. (Original) The program update method of claim 1, wherein:
the LSI device includes a boot ROM in which a boot program is stored;
the external memory includes an acquisition program for establishing data transmission between the LSI device and a server; and
the system executes reception of the common key-encrypted program based on the acquisition program stored in the external memory, and controls update processing performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM.

8. (Previously presented) The program update method of claim 1, further comprising the step of receiving a HASH value of the raw program transmitted from the server,
wherein at the decrypting step, the received HASH value is used to perform a HASH verification on the decrypted raw program.

9-11. (Cancelled)